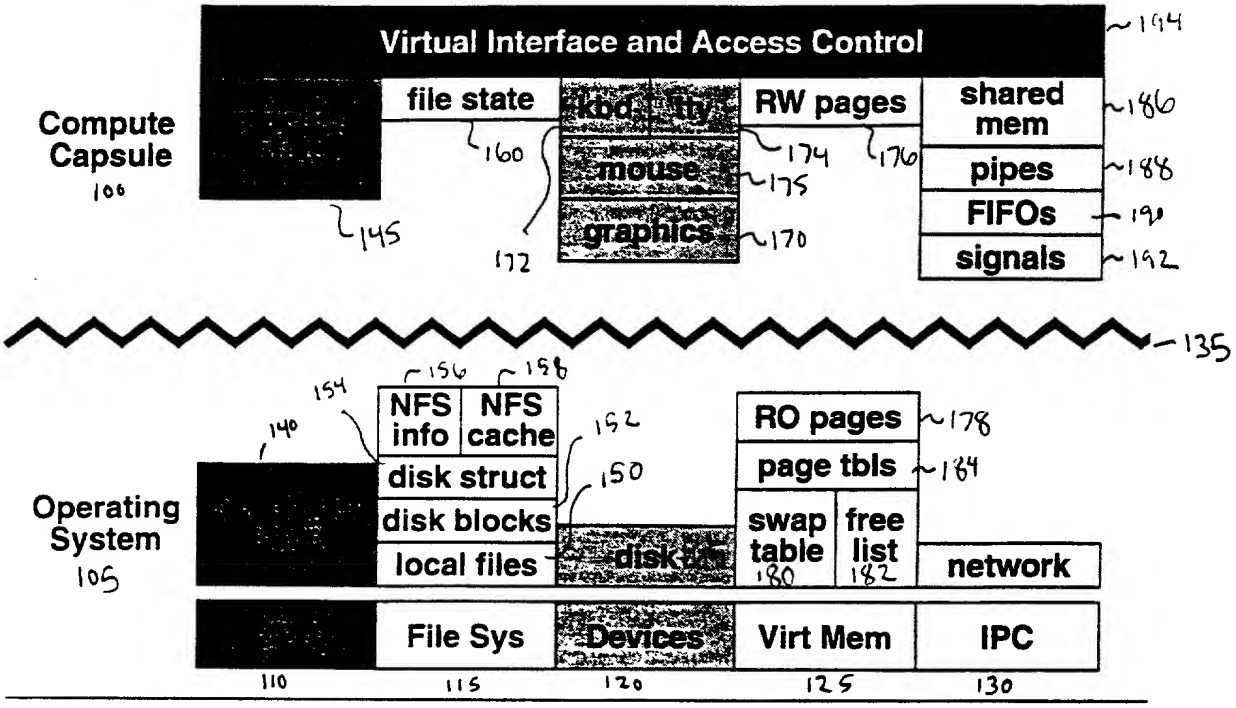

Virtual Interface and Access Control
194
Compute Capsule
100
file state
kbd
fty
RW pages
shared mem
186
160
174
176
mouse
175
pipes
188
145
172
graphics
170
FIFOs
190
signals
192
135
154
156
158
NFS info
NFS cache
140
152
RO pages
178
page tbls
184
Operating System
105
disk struct
150
disk blocks
swap table
180
free list
182
local files
disk drv
network
File Sys
Devices
Virt Mem
IPC
110
115
120
125
130

Figure 1

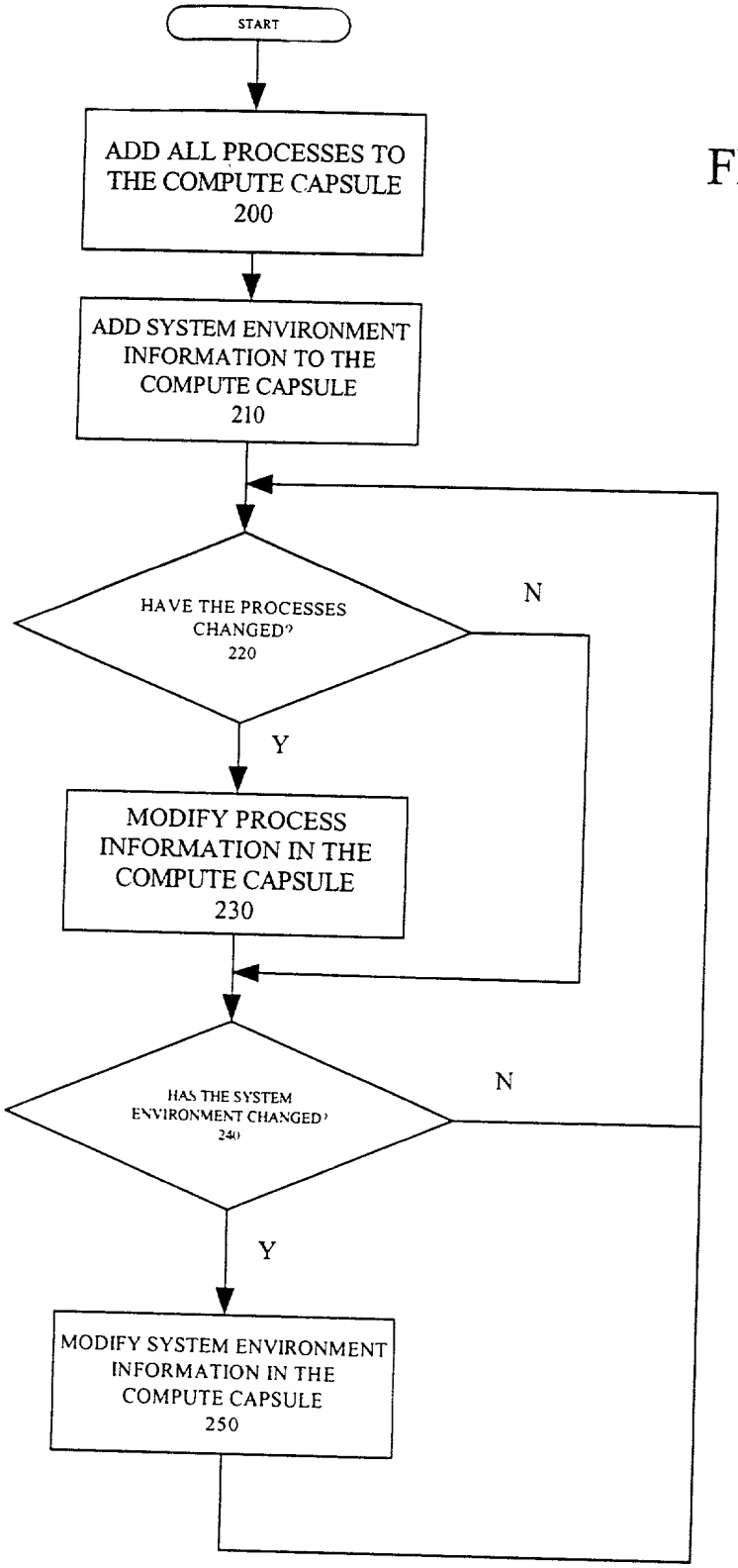

START
ADD ALL PROCESSES TO THE COMPUTE CAPSULE 200
ADD SYSTEM ENVIRONMENT INFORMATION TO THE COMPUTE CAPSULE 210
HAVE THE PROCESSES CHANGED? 220
N
Y
MODIFY PROCESS INFORMATION IN THE COMPUTE CAPSULE 230
HAS THE SYSTEM ENVIRONMENT CHANGED? 240
N
Y
MODIFY SYSTEM ENVIRONMENT INFORMATION IN THE COMPUTE CAPSULE 250

FIGURE 2

FIGURE 3A

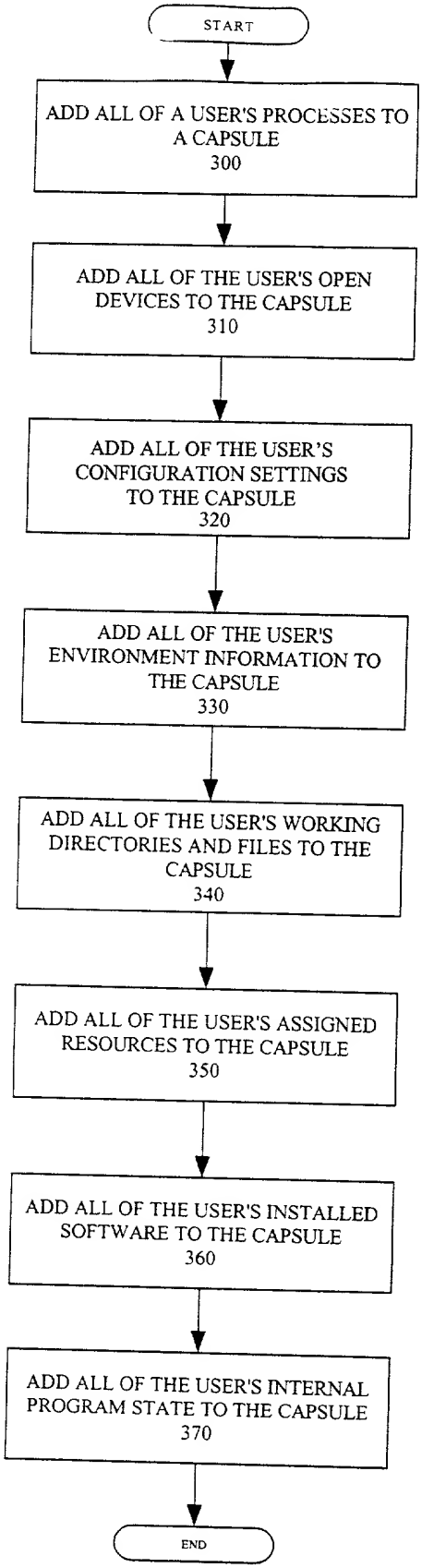
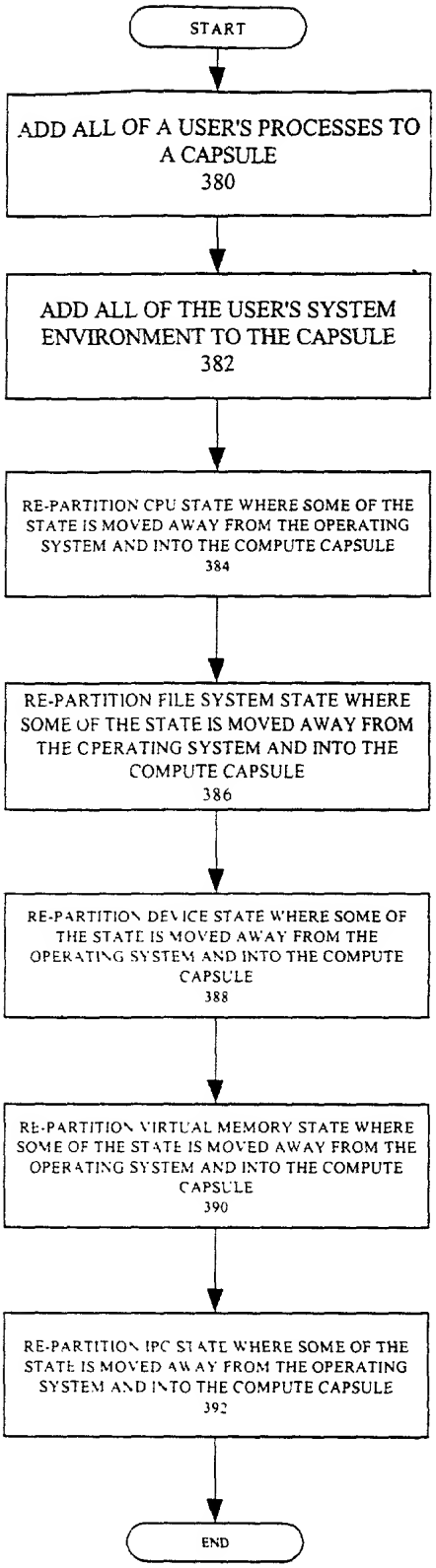

START
ADD ALL OF A USER'S PROCESSES TO A CAPSULE
300
ADD ALL OF THE USER'S OPEN DEVICES TO THE CAPSULE
310
ADD ALL OF THE USER'S CONFIGURATION SETTINGS TO THE CAPSULE
320
ADD ALL OF THE USER'S ENVIRONMENT INFORMATION TO THE CAPSULE
330
ADD ALL OF THE USER'S WORKING DIRECTORIES AND FILES TO THE CAPSULE
340
ADD ALL OF THE USER'S ASSIGNED RESOURCES TO THE CAPSULE
350
ADD ALL OF THE USER'S INSTALLED SOFTWARE TO THE CAPSULE
360
ADD ALL OF THE USER'S INTERNAL PROGRAM STATE TO THE CAPSULE
370
END

FIGURE 3B


START
ADD ALL OF A USER'S PROCESSES TO A CAPSULE
380
ADD ALL OF THE USER'S SYSTEM ENVIRONMENT TO THE CAPSULE
382
RE-PARTITION CPU STATE WHERE SOME OF THE STATE IS MOVED AWAY FROM THE OPERATING SYSTEM AND INTO THE COMPUTE CAPSULE
384
RE-PARTITION FILE SYSTEM STATE WHERE SOME OF THE STATE IS MOVED AWAY FROM THE CPERATING SYSTEM AND INTO THE COMPUTE CAPSULE
386
RE-PARTITION DEVICE STATE WHERE SOME OF THE STATE IS MOVED AWAY FROM THE OPERATING SYSTEM AND INTO THE COMPUTE CAPSULE
388
RE-PARTITION VIRTUAL MEMORY STATE WHERE SOME OF THE STATE IS MOVED AWAY FROM THE OPERATING SYSTEM AND INTO THE COMPUTE CAPSULE
390
RE-PARTITION IPC STATE WHERE SOME OF THE STATE IS MOVED AWAY FROM THE OPERATING SYSTEM AND INTO THE COMPUTE CAPSULE
392
END

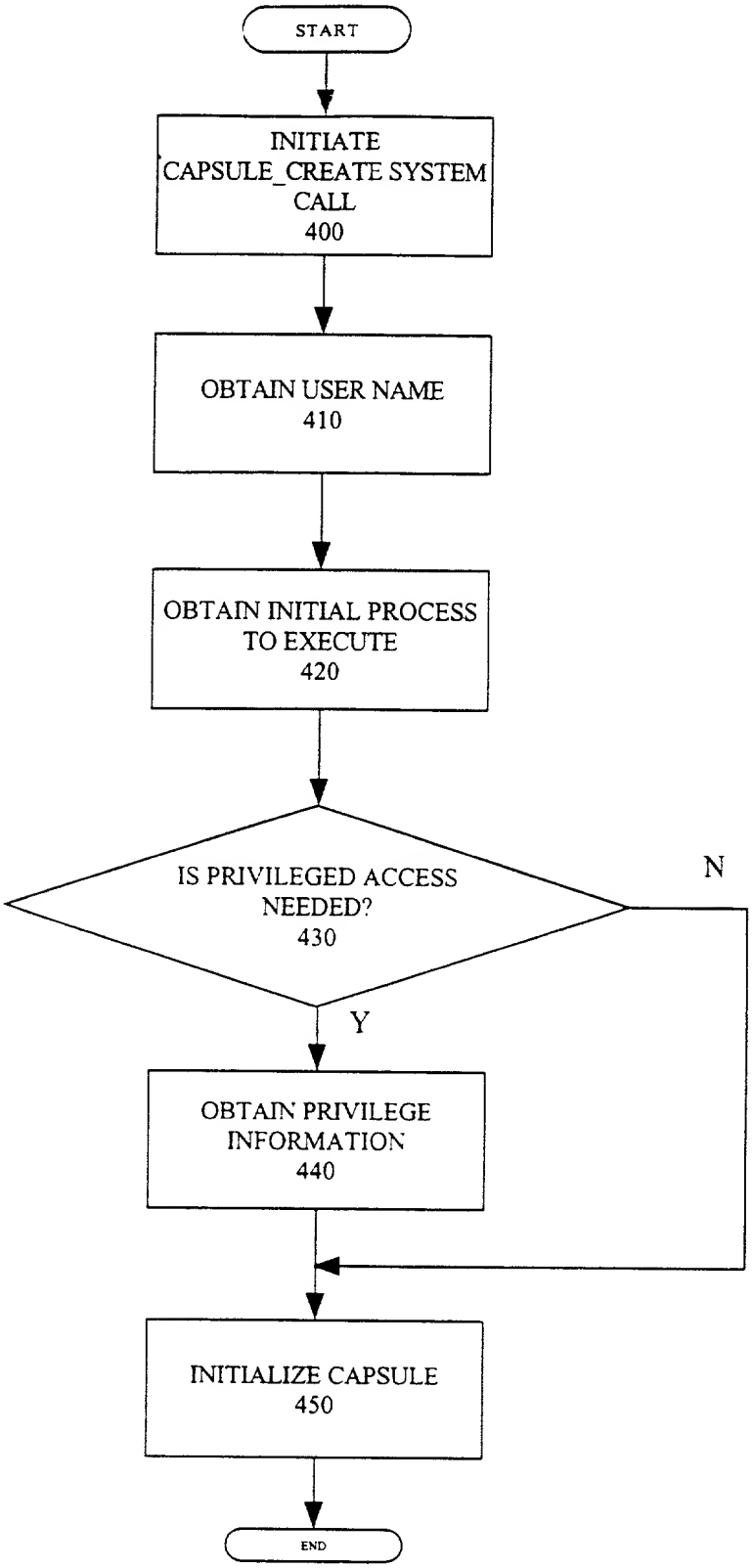

START
INITIATE CAPSULE_CREATE SYSTEM CALL 400
OBTAIN USER NAME 410
OBTAIN INITIAL PROCESS TO EXECUTE 420
IS PRIVILEGED ACCESS NEEDED? 430
N
Y
OBTAIN PRIVILEGE INFORMATION 440
INITIALIZE CAPSULE 450
END

FIGURE 4

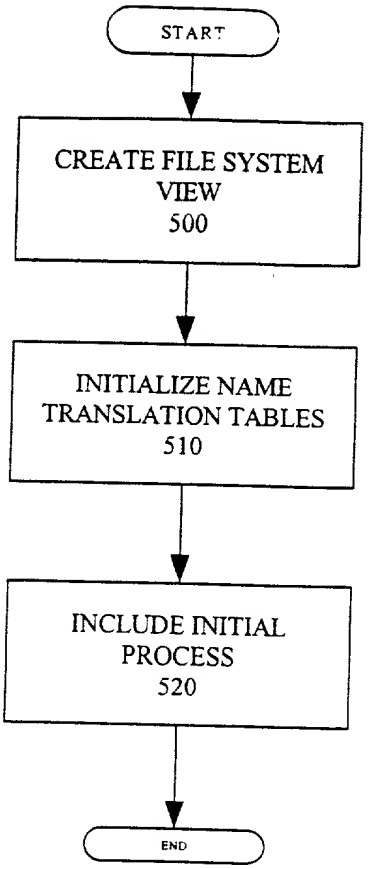

START
CREATE FILE SYSTEM VIEW 500
INITIALIZE NAME TRANSLATION TABLES 510
INCLUDE INITIAL PROCESS 520
END

FIGURE 5

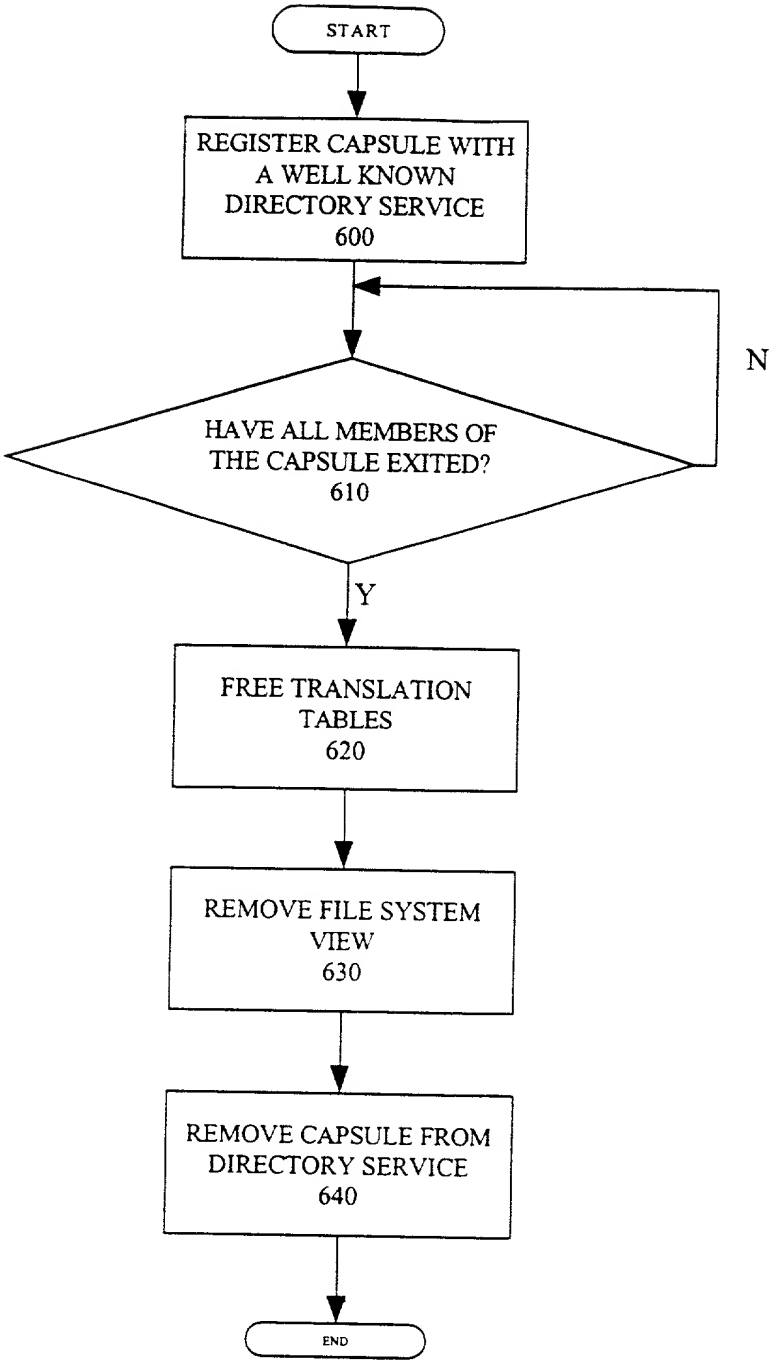

START
REGISTER CAPSULE WITH A WELL KNOWN DIRECTORY SERVICE 600
HAVE ALL MEMBERS OF THE CAPSULE EXITED? 610
N
Y
FREE TRANSLATION TABLES 620
REMOVE FILE SYSTEM VIEW 630
REMOVE CAPSULE FROM DIRECTORY SERVICE 640
END

FIGURE 6

FIGURE 7

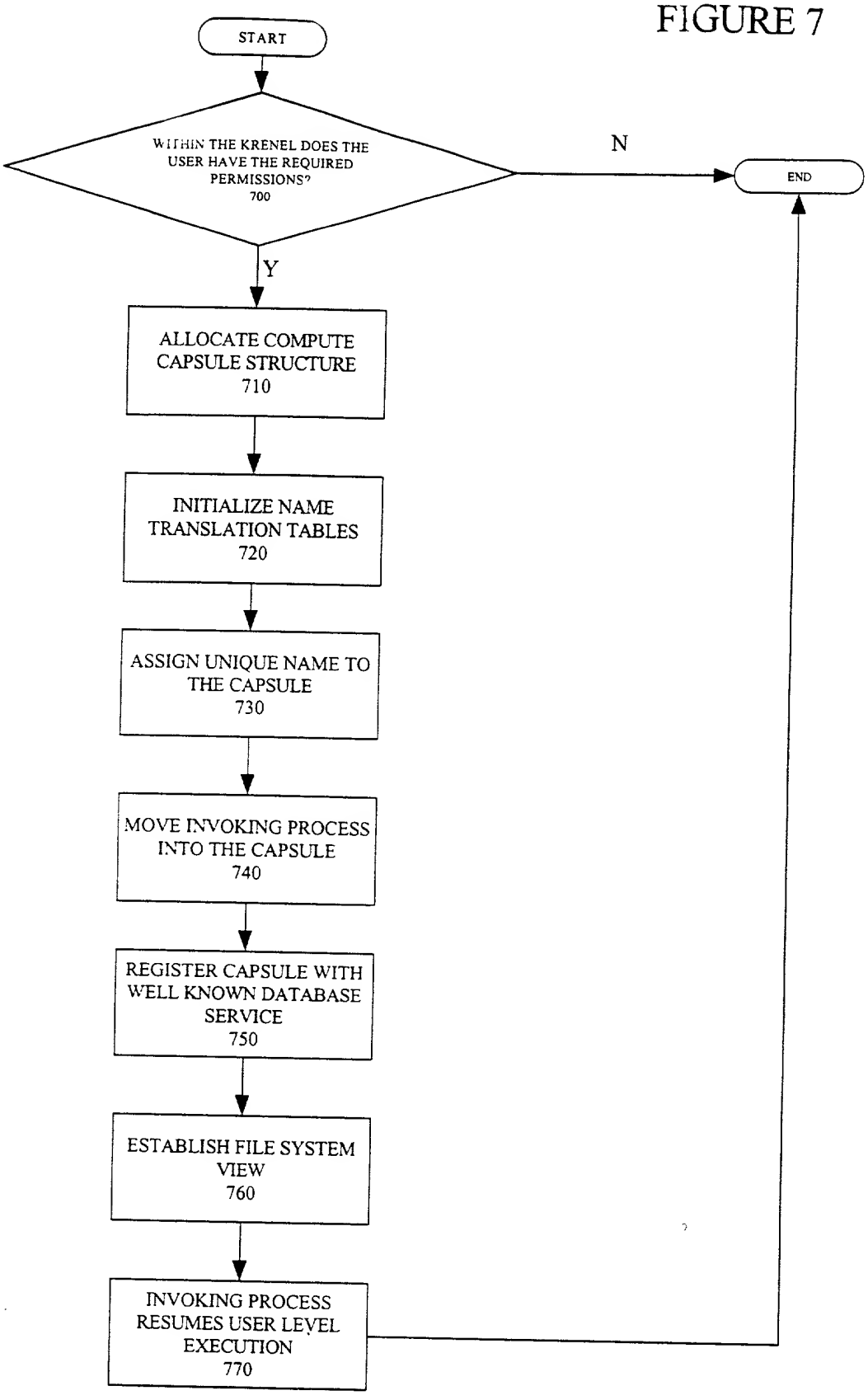

START
WITHIN THE KRENEL DOES THE USER HAVE THE REQUIRED PERMISSIONS?
700
N
END
Y
ALLOCATE COMPUTE CAPSULE STRUCTURE
710
INITIALIZE NAME TRANSLATION TABLES
720
ASSIGN UNIQUE NAME TO THE CAPSULE
730
MOVE INVOKING PROCESS INTO THE CAPSULE
740
REGISTER CAPSULE WITH WELL KNOWN DATABASE SERVICE
750
ESTABLISH FILE SYSTEM VIEW
760
INVOKING PROCESS RESUMES USER LEVEL EXECUTION
770

FIGURE 8

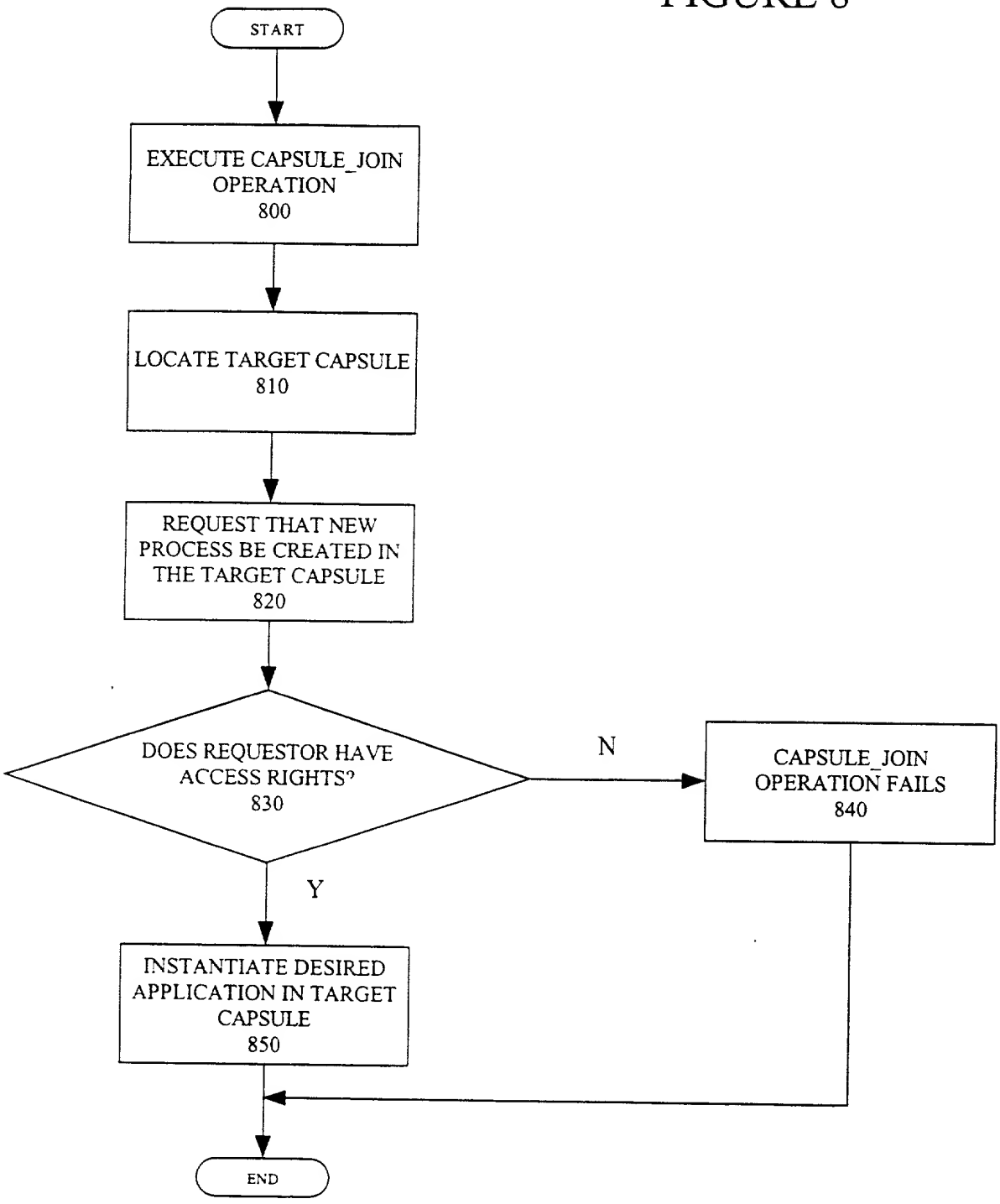
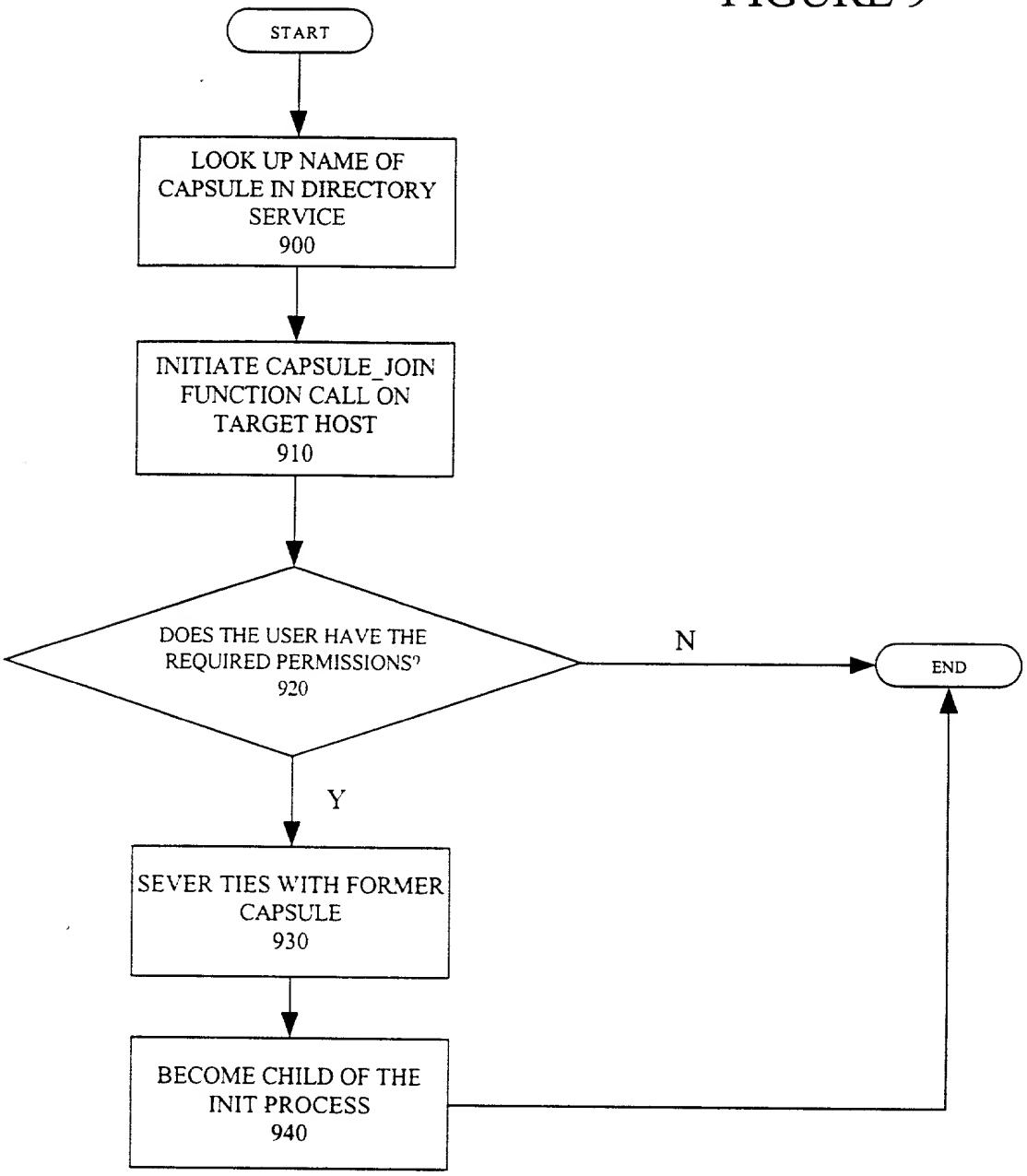

START
EXECUTE CAPSULE_JOIN OPERATION 800
LOCATE TARGET CAPSULE 810
REQUEST THAT NEW PROCESS BE CREATED IN THE TARGET CAPSULE 820
DOES REQUESTOR HAVE ACCESS RIGHTS? 830
N
CAPSULE_JOIN OPERATION FAILS 840
Y
INSTANTIATE DESIRED APPLICATION IN TARGET CAPSULE 850
END

FIGURE 9


START
LOOK UP NAME OF CAPSULE IN DIRECTORY SERVICE
900
INITIATE CAPSULE_JOIN FUNCTION CALL ON TARGET HOST
910
DOES THE USER HAVE THE REQUIRED PERMISSIONS?
920
N
END
Y
SEVER TIES WITH FORMER CAPSULE
930
BECOME CHILD OF THE INIT PROCESS
940

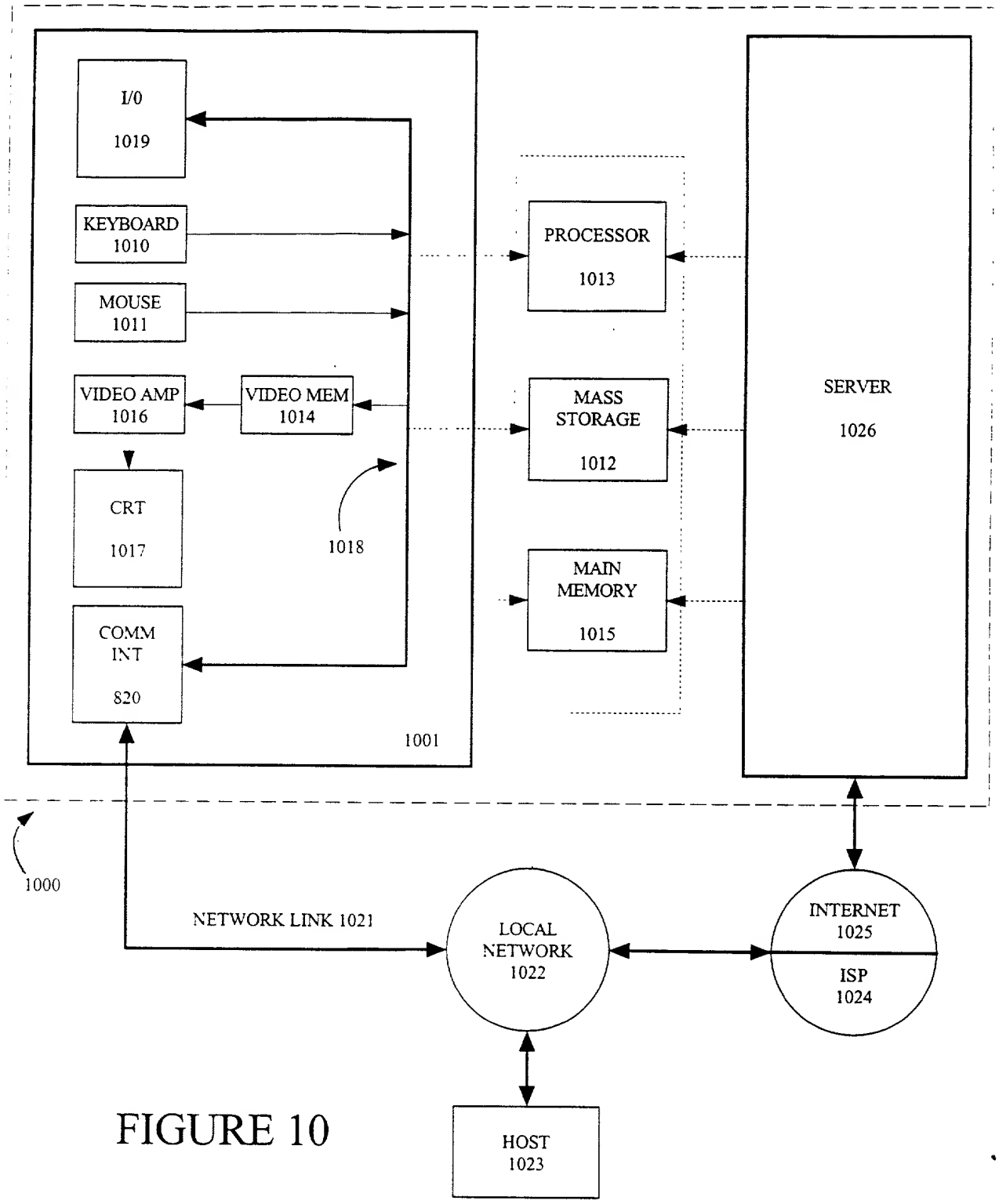

I/O
1019
KEYBOARD
1010
MOUSE
1011
VIDEO AMP
1016
VIDEO MEM
1014
CRT
1017
1018
COMM
INT
820
1001
PROCESSOR
1013
MASS
STORAGE
1012
MAIN
MEMORY
1015
SERVER
1026
1000
NETWORK LINK 1021
LOCAL
NETWORK
1022
INTERNET
1025
ISP
1024
HOST
1023

FIGURE 10

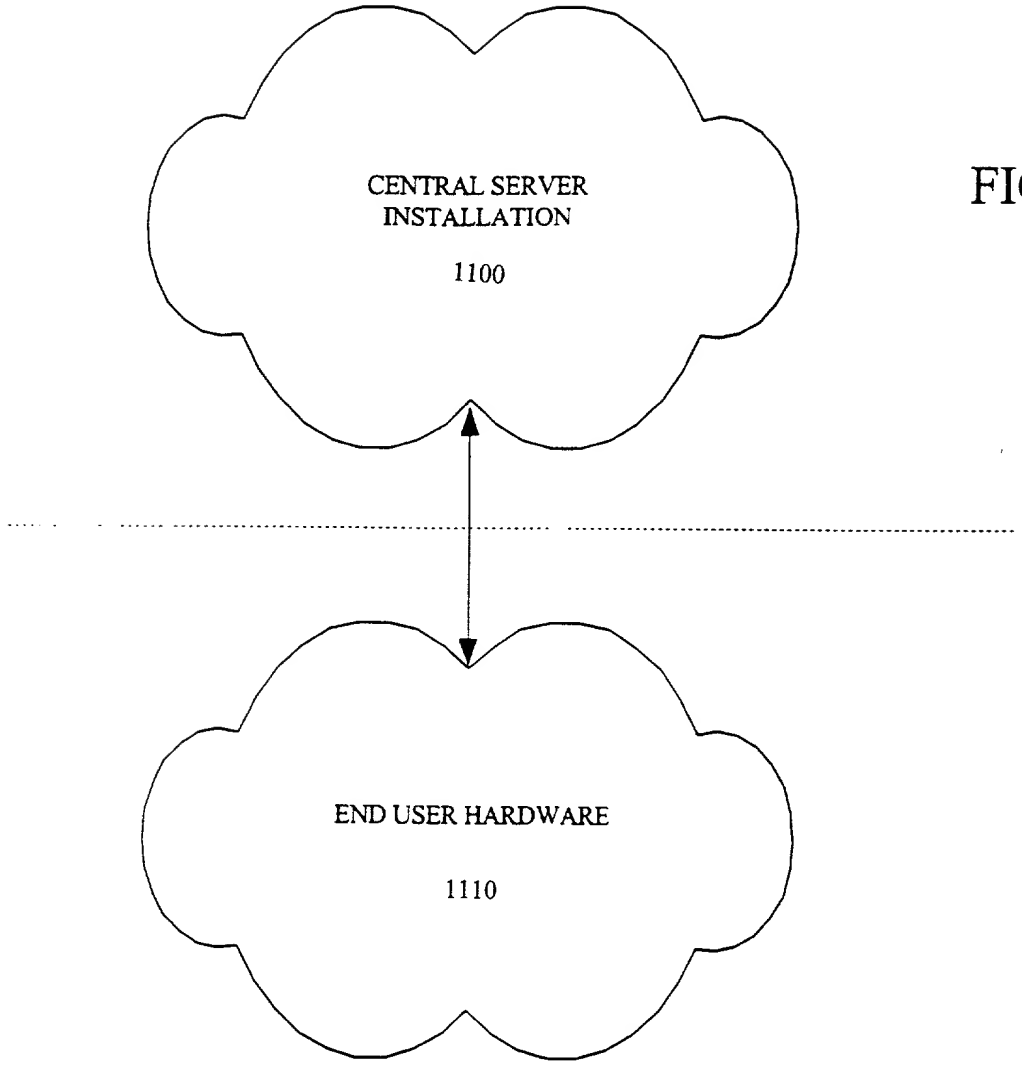


FIGURE 11

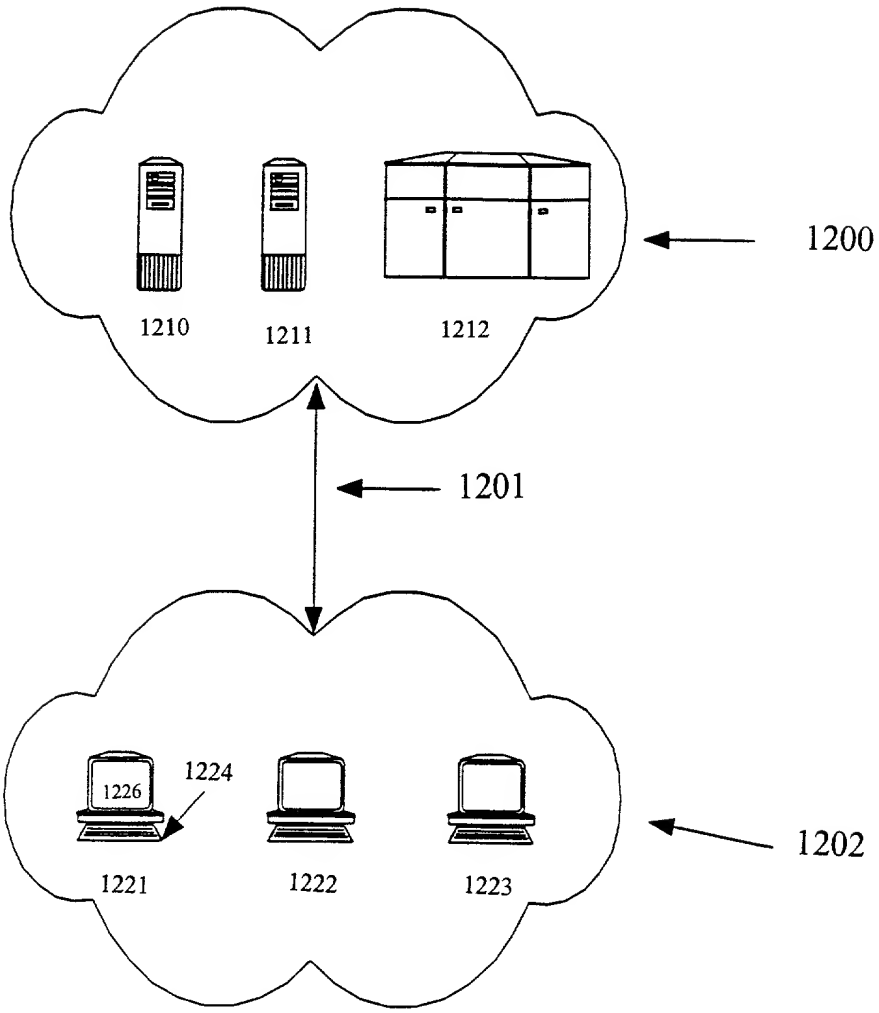


FIGURE 12

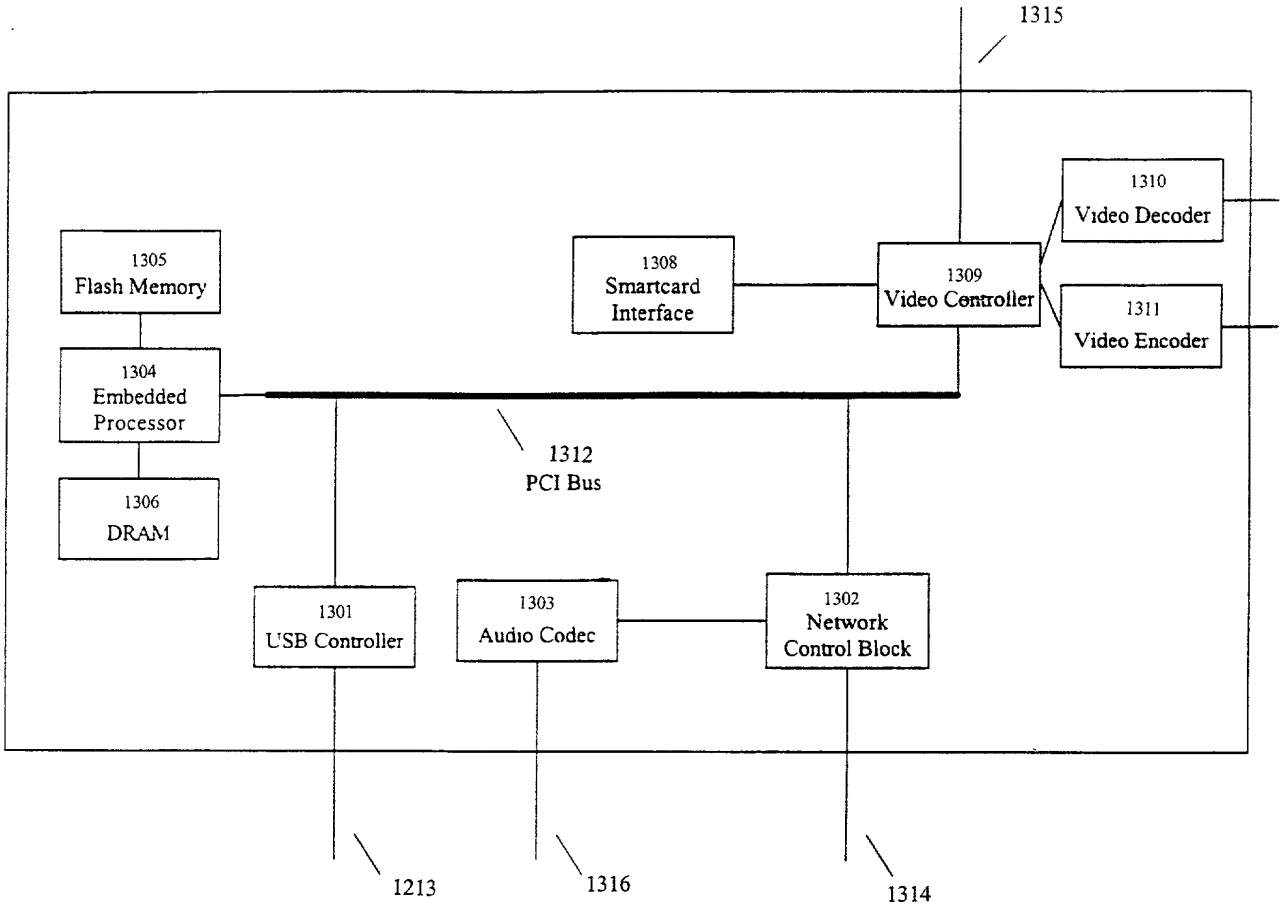


Figure13: HID

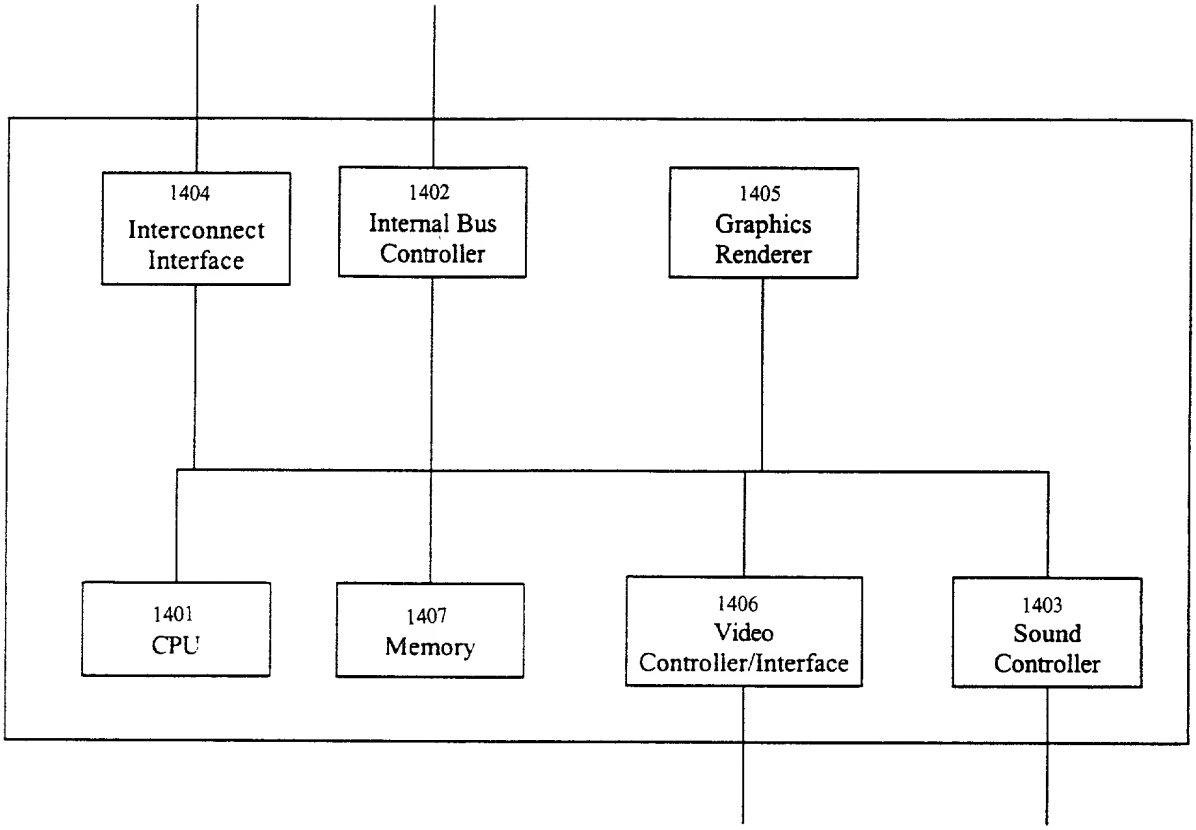


Figure 14: HID Single Chip Implementation

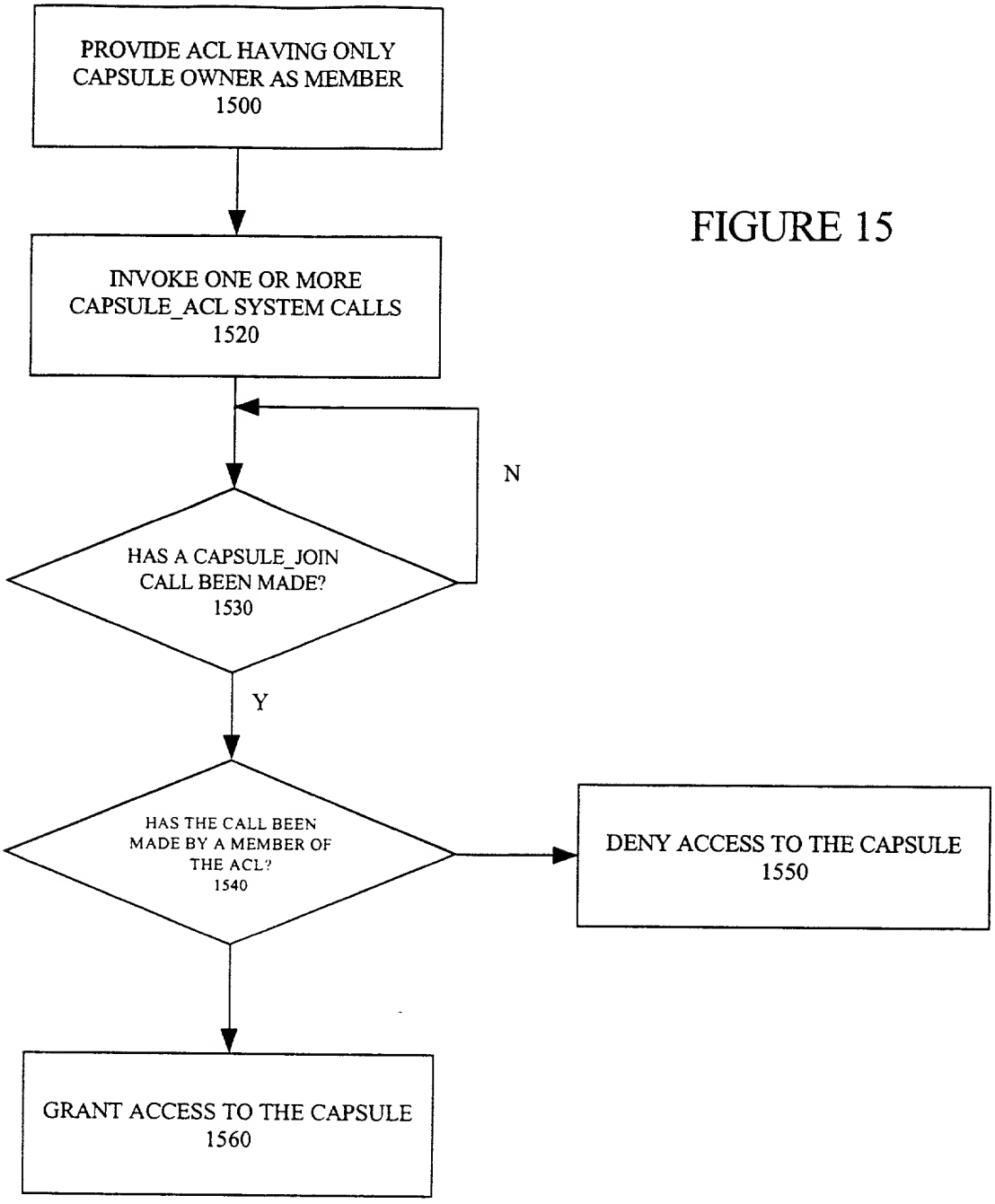

PROVIDE ACL HAVING ONLY CAPSULE OWNER AS MEMBER 1500
INVOKE ONE OR MORE CAPSULE_ACL SYSTEM CALLS 1520
HAS A CAPSULE_JOIN CALL BEEN MADE? 1530
N
Y
HAS THE CALL BEEN MADE BY A MEMBER OF THE ACL? 1540
DENY ACCESS TO THE CAPSULE 1550
GRANT ACCESS TO THE CAPSULE 1560

FIGURE 15